UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/797,849	03/10/2004	Brig Barnum Elliott	03-4029	5647

7590 07/26/2007

Verizon Corporate Services Group Inc.
Mail Code: HQE03H14
600 Hidden Ridge Drive
Irving, TX 75038

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
07/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/797,849	ELLIOTT, BRIG BARNUM	
	Examiner	Art Unit	
	Jung Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15 and 17-42* is/are rejected.

7)☒ Claim(s) *16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *see enclosed*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-42 are pending.

Information Disclosure Statement

2. The IDS submitted on 3/10/04 has been considered. An initialed copy is enclosed.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-8, 12-14, 17-20, 22, 23, 25-29, 31-35 and 42 are rejected under 35 U.S.C. 102(e) as being anticipated by Azuma et al. USPN 7,035,411 (hereinafter Azuma).

5. As per claims 1-8, 12-14 and 17, Azuma discloses a method of authenticating an optical channel comprising:

a. modulating optical pulses corresponding to a first bit sequence based on a second bit sequence; (fig. 15, "N-Qubit quantum information", "N-bit string", "random 2n-bit string", "random 4N-bit string"; fig. 16, N-Qubit quantum information", "2N-bit string", "random Log[(m+n)!]-bit string", "M-bit string")

b. transmitting the modulated optical pulses over the optical channel; receiving the modulated optical pulses; ("Quantum channel")

c. demodulating the received modulated optical pulses using the second bit sequence; ("1st password" and "2nd password") and

d. authenticating the optical channel based on a number of bits from the first bit sequence that are correctly received and demodulated; (figs. 15, 16: reference nos. 1522, 1523, 1524, 1622, 1623 and 1624)

e. wherein every bit in the first bit sequence is identical; (fig. 15, 16: "signature"; there exists at least one subset of the digital signature wherein every bit of the subset are identical)

f. wherein the first bit sequence is a pseudo-random bit sequence; wherein the second bit sequence is a pseudo-random bit sequence; (col. 9:54-67; 10:5-7)

g. wherein the optical pulses are modulated using polarization modulation; wherein each bit of the first bit sequence specifies one of two possible polarizations to apply to the optical pulses; wherein each K bits of the second bit sequence, where K is a positive integer, specifies a polarization to apply to the optical pulses; wherein each bit of the first bit sequence specifies either a vertical or horizontal polarization; (col. 6:25-27; 28:26-29:30)

h. wherein authenticating the optical channel includes:

i. tabulating the number of bits from the first bit sequence that are correctly received; tabulating the number of bits from the first bit sequence that are incorrectly received; and authenticating the optical channel when the tabulated number of correctly received bits expressed as a fraction of a total number of correctly and incorrectly received bits is greater than a threshold value; (col. 27:19-28:24)

i. wherein the first bit sequence and the second bit sequence are derived from shared secret keys; (fig. 15 and 16: "1st Password" "2nd Password" "signature")

j. wherein the second bit sequence is distributed as a shared secret key and the first bit sequence is distributed as a known sequence; (Quantum Channel is observed)

k. sharing the second bit sequence over a public channel, wherein authenticating the optical channel further includes
transmitting a representation of the demodulated and received optical pulses to an entity that transmitted the optical pulses over the optical channel, and comparing the first bit sequence to the representation of the demodulated and received optical pulses. (fig. 15, reference no. 1523, "To Alice"; fig. 16, reference no. 1623, "To Alice")

6. As per claims 18-20, 22 and 23, they are claims corresponding to claims 1-8, 12-14 and 17, and they do not teach or define above the information claimed in claims 1-8, 12-14 and 17. Therefore, claims 18-20, 22 and 23 are rejected as being anticipated by Azuma over for the same reasons set forth in the rejections of claims 1-8, 12-14 and 17.

7. As per claims 25-29, Azuma discloses a cryptographic device comprising:

l. a polarized pulse generator configured to emit optical pulses polarized in one of a first state and a second state based on values stored in a first bit sequence; and a polarizing rotator configured to rotate the optical pulses received from the polarized pulse generator by an angle specified by one or more bits from a second bit sequence to obtain a series of modulated optical pulses, (col. 6:25-27)

m. wherein the optical pulses are transmitted over an optical channel and used to authenticate the optical channel; (figs. 15 and 16 "Quantum Channel")

n. wherein the polarized pulse generator further comprises: a first laser configured to emit a horizontally polarized optical pulse when a bit in the first bit sequence specifies the first state; and a second laser configured to emit a vertically polarized optical pulse when the bit in the first bit sequence specifies the second state; wherein each bit of the first bit sequence specifies either a vertical or horizontal polarization; figs. 15 and 16, "generator"; 6:27: "rectilinear basis")

o. wherein the first bit sequence and the second bit sequence are distributed as shared secret keys; (fig. 15 and 16: "1st Password" "2nd Password" "signature")

p. wherein the second bit sequence is distributed as a shared secret key and the first bit sequence is distributed as a known sequence. (Channel is observed)

8. As per claims 31-35, Azuma discloses a cryptographic device comprising:

q. a polarization rotator configured to rotate optical pulses received over an optical channel by an angle specified by one or more bits from a second bit sequence; and (col. 6:25-27)

r. a polarizing beam splitter configured to receive the optical pulses rotated by the polarization rotator; a detector configured to generate indications of the polarizations of the received optical pulses; (fig. 12a and 12c) and

s. a counter configured to tabulate a number of times the detector indicates that the received optical pulses are polarized in a state that matches a state of a corresponding bit in a first bit sequence, wherein the optical channel is authenticated based on at least one count value of the counter; wherein the counter is further configured to tabulate a number of times the detector indicates that the received optical pulses are polarized in a state that does not match the state of the corresponding bit in the first bit sequence; (col. 28:19-24)

t. wherein each bit of the first bit sequence specifies either a vertical or horizontal polarization; (col. 6:25-27)

u. wherein the first bit sequence and the second bit sequence are distributed as shared secret keys; (fig. 15 and 16: "1st Password" "2nd Password" "signature")

v. wherein the second bit sequence is distributed as a shared secret key and the first bit sequence is distributed as a known sequence. (Channel is observed)

9. As per claim 42, Azuma discloses a device comprising:

w. means for receiving optical pulses corresponding to a first bit sequence that were modulated based on a second bit sequence, the optical pulses being received over an optical channel; (fig. 15, "N-Qubit quantum information", "N-bit string", "random 2n-bit string", "random 4N-bit string"; fig. 16, N-Qubit quantum information", "2N-bit string", "random Log[(m+n)!]-bit string", "M-bit string"; "Quantum Channel")

x. means for demodulating the received optical pulses using the second bit sequence; ("1st password" and "2nd password") and

y. means for authenticating the optical channel based on a number of bits from the first bit sequence that are correctly received and demodulated. (figs. 15, 16: reference nos. 1522, 1523, 1524, 1622, 1623 and 1624)

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 9-11, 21 and 37-40 are rejected under 35 USC 103(a) as being unpatentable over Azuma in view of Lutkenhaus US Patent Application Publication No. 20040151321 (hereinafter Lutkenhaus).

12. As per claims 9-11, the rejections of claims 5-7 under 35 USC 102(e) as being unpatentable over Azuma is incorporated herein. Azuma does not expressly disclose wherein the optical pulses are modulated using phase modulation; wherein each bit of the first bit sequence specifies one of two possible phases to shift the optical pulses; wherein each K bits of the second bit sequence, where K is a positive integer, specifies a phase to shift the optical pulses. Lutkenhaus discloses it is well established in the art to use either polarizations or phases of a photon to define quantum states (Paragraph 5). For example, the original BB84 uses polarizations of a photo whereas optical fibre based implementations of BB84 utilize phase states. (Paragraphs 6-10) It would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Azuma to be modified so that the optical pulses are modulated using phase modulation; wherein each bit of the first bit sequence specifies one of two possible phases to shift the optical pulses; wherein each K bits of the second bit sequence, where K is a positive integer, specifies a phase to shift the optical pulses. One would be motivated to do so to use phase modulations in optical communications because polarization and phase modulations are the two basic categories of effective orthogonal

states as known to one of ordinary skill in the art. Lutkenhaus, paragraph 5. The aforementioned cover the limitations of claims 9-11.

13. As per claim 21, it is a claim corresponding to claims 9-11 and 18, and it does not teach or define above the information claimed in claims 9-11 and 18. Therefore, claim 21 is rejected as being unpatentable over Azuma in view of Lutkenhaus for the same reasons set forth in the rejections of claims 9-11 and 18.

14. As per claims 37-40, the rejections of claims 25-29 under 35 USC 102(e) as being anticipated by Azuma is incorporated herein. Azuma does not disclose using phase modulation to define the quantum states. Lutkenhaus discloses it is well established in the art to use either polarizations or phases of a photon to define quantum states (Paragraph 5). For example, the original BB84 uses polarizations of a photon whereas optical fibre based implementations of BB84 utilize phase states. (Paragraphs 6-10) It would be obvious to one of ordinary skill in the art at the time the invention was made for the invention of Azuma to be modified so that the optical pulses are modulated using phase modulation such that the invention includes phase setting logic configured to determine an initial phase based on values stored in a first bit sequence; summing logic configured to add the initial phase to a second phase determined based on one or more bits from a second bit sequence and to output a summed phase angle; and a phase modulator configured to modulate optical pulses by the summed phase angle to obtain a series of modulated optical pulses,

wherein the modulated optical pulses are transmitted over an optical channel and used to authenticate the optical channel; and a photon source configured to generate the optical pulses. One would be motivated to do so to use phase modulations in optical communications because polarization and phase modulations are the two basic categories of effective orthogonal states as known to one of ordinary skill in the art. Lutkenhaus, paragraph 5. The aforementioned cover the limitations of claims 37-40.

15. Claims 15, 24, 30 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Azuma in view of Newcombe et al. USPN 7,243,226 (hereinafter Newcombe).

16. As per claim 15, the rejection of claim 1 under 35 USC 102(e) as being anticipated by Azuma is incorporated herein. Azuma discloses using a digital signature as the first bit sequence (col. 7:10-14), but Azuma does not disclose computing a message authentication code based on communications over a public channel; and deriving at least one of the first and second bit sequences based on the message authentication code. However, in the cryptographic art, MACs are traditionally used with or in place of digital signatures. For example, Newcombe discloses a method and system for enabling content security in a distributed system whereby a client and server utilize a HMAC and/or a digital signature to authenticate the transmission as well as to authenticate the participants of the transmission. Col. 3:66-4:14. It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention

of Azuma by computing a MAC based on communications over a public channel; and deriving at least one of the first and second bit sequences based on the MAC. One would be motivated to do so to provide a robust means of authenticating the parties as known to one of ordinary skill in the art and as taught by Newcombe, ibid. The aforementioned cover the limitations of claim 15.

17. As per claim 24, it is a claim corresponding to claims 15 and 18, and it does not teach or define above the information claimed in claims 15 and 18. Therefore, claim 24 is rejected as being unpatentable over Azuma in view of Newcombe for the same reasons set forth in the rejections of claims 15 and 18.

18. As per claim 30, it is a claim corresponding to claims 15 and 25, and it does not teach or define above the information claimed in claims 15 and 25. Therefore, claim 30 is rejected as being unpatentable over Azuma in view of Newcombe for the same reasons set forth in the rejections of claims 15 and 25.

19. As per claim 36, it is a claim corresponding to claims 15 and 31, and it does not teach or define above the information claimed in claims 15 and 31. Therefore, claim 36 is rejected as being unpatentable over Azuma in view of Newcombe for the same reasons set forth in the rejections of claims 15 and 31.

20. Claim 41 is rejected under 35 U.S.C. 103(a) as being unpatentable over Azuma in view of Newcombe and further in view of Lutkenhaus.

21. As per claim 41, the rejection of claim 37 under 35 USC 103(a) as being unpatentable over Azuma in view of Newcombe is incorporated herein. Azuma discloses using a digital signature as the first bit sequence (col. 7:10-14), but Azuma does not disclose computing a message authentication code based on communications over a public channel; and deriving at least one of the first and second bit sequences based on the message authentication code. However, in the cryptographic art, MACs are traditionally used with or in place of digital signatures. For example, Newcombe discloses a method and system for enabling content security in a distributed system whereby a client and server utilize a HMAC and/or a digital signature to authenticate the transmission as well as to authenticate the participants of the transmission. Col. 3:66-4:14. It would be obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Azuma by computing a MAC based on communications over a public channel; and deriving at least one of the first and second bit sequences based on the MAC. One would be motivated to do so to provide a robust means of authenticating the parties as known to one of ordinary skill in the art and as taught by Newcombe, ibid. The aforementioned cover the limitations of claim 41.

Allowable Subject Matter

22. Claim 16 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132